(19)日本国特許庁（ＪＰ）　(12) **公開特許公報（Ａ）**　(11)特許出願公開番号
特開2002－244756
（P2002－244756A）
(43)公開日　平成14年８月30日(2002.8.30)

(51)Int.Cl.[7]	識別記号	ＦＩ		テーマコード（参考）
Ｇ０６Ｆ　1/00		Ｃ０６Ｋ　17/00	Ｄ	５Ｂ０３５
Ｇ０６Ｋ　17/00			Ｅ	５Ｂ０５８
		Ｇ０９Ｃ　1/00	６４０Ａ	５Ｂ０７６
19/07		Ｇ０６Ｆ　9/06	６６０Ｃ	５Ｊ１０４
19/073			６６０Ｊ	

審査請求　未請求　請求項の数20　ＯＬ　（全 14 頁）　最終頁に続く

(21)出願番号　特願2001－42396(P2001－42396)

(22)出願日　平成13年２月19日(2001.2.19)

(71)出願人　000002185
ソニー株式会社
東京都品川区北品川６丁目７番35号

(72)発明者　末吉　正弘
東京都品川区北品川６丁目７番35号　ソニー株式会社内

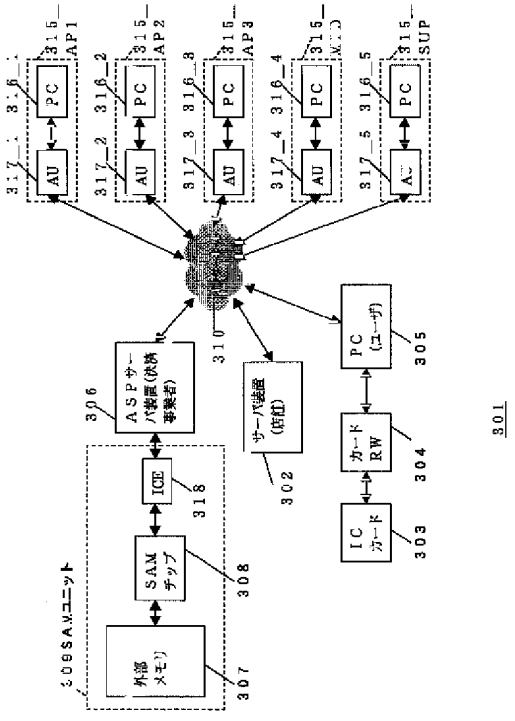
(72)発明者　久保野　文夫
東京都品川区北品川６丁目７番35号　ソニー株式会社内

(74)代理人　100094053
弁理士　佐藤　隆久

最終頁に続く

(54)【発明の名称】　データ処理方法、半導体回路および認証用装置

(57)【要約】
【課題】　サーバ装置などの半導体回路へのアクセス内容をその権限に応じて規制できるデータ処理方法を提供する。
【解決手段】　ＳＡＭチップ３０８が、複数の階層からなるソフトウェア構造を有し、各階層に対応したダウンロード用署名検証鍵情報参照可能である。ＳＡＭチップ３０８がパーソナルコンピュータ３１６＿１からダウンロード要求を受けると、認証用ユニット３１７＿１において、ダウンロード用署名情報を作成し、これがＳＡＭチップ３０８に送信される。ＳＡＭチップ３０８では、ダウンロード用署名検証鍵情報を用いて、受信したダウンロード用署名情報を検証し、正当であると判断した場合にダウンロードを認める。



【特許請求の範囲】
【請求項１】半導体回路または当該半導体回路がアクセス可能な半導体記憶装置に、前記半導体回路内で動作するプログラムをダウンロードするデータ処理方法において、
前記半導体回路が複数の階層からなるソフトウェア構造を有し、各階層に対応したダウンロード用署名検証鍵情報を前記半導体回路が参照可能であり、
前記半導体回路がダウンロード要求を受けると、当該ダウンロード要求に対応して生成されたダウンロード用署名情報を、前記ダウンロード用署名検証鍵情報を用いて検証し、
前記ダウンロード用署名情報が正当であると検証したことを条件に、当該検証に用いたダウンロード用署名検証鍵情報に対応した階層プログラムのダウンロードを、前記ダウンロード要求の発行元に許可するデータ処理方法
【請求項２】認証用装置が、ダウンロードが許可されるプログラムが属する階層に対応したアクセス原鍵情報を記憶し、
前記認証用装置が、前記半導体回路に前記ダウンロード要求を送信し、
前記認証用装置が、当該アクセス原鍵情報を用いて前記ダウンロード用署名情報を生成し、当該ダウンロード用署名情報を前記半導体回路に送信する請求項１に記載のデータ処理方法。
【請求項３】前記認証用装置が、前記半導体回路の識別情報を記憶し、
前記認証用装置が、前記識別情報を平文として前記アクセス原鍵情報を用いて暗号化を行ってダウンロード用源鍵情報を生成し、当該ダウンロード用原鍵情報を用いて前記ダウンロード用署名情報を生成する請求項２に記載のデータ処理方法。
【請求項４】前記認証用装置が、前記半導体回路へのダウンロードを許可された前記階層に対応する第１のアクセス原鍵情報、並びに、当該階層の上位の単数または複数の階層にそれぞれ対応した単数または複数の第２のアクセス原鍵情報を記憶し、
前記認証用装置が、前記第１のアクセス原鍵情報、並びに前記単数または複数の第２のアクセス原鍵情報を用いて前記ダウンロード用署名情報を生成する請求項２に記載のデータ処理方法。
【請求項５】前記認証用装置は、前記半導体回路との間で相互認証を行った後に、前記ダウンロード用署名情報を前記半導体回路に送信する請求項２に記載のデータ処理方法。
【請求項６】前記認証用装置が、相互認証用原鍵情報、並びに前記半導体回路の識別情報を記憶し、
前記認証用装置が、前記識別情報を平文として前記相互認証用原鍵情報を用いて暗号化を行って相互認証用鍵情報を生成し、
前記認証用装置が、前記相互認証用鍵情報を用いて前記半導体回路との間で相互認証を行う請求項５に記載のデータ処理方法。
【請求項７】前記半導体回路のソフトウェア構造が、前記半導体回路の管理者にのみダウンロード権が与えられた第１の階層と、前記第１の階層の上位に位置し所定の集積回路を操作するプログラムが属する第２の階層と、前記第２の階層の上位に位置し前記集積回路を用いた取り引き手続き内容を規定したアプリケーションプログラムが属する第３の階層とに分類されている請求項１に記載のデータ処理方法。
【請求項８】前記集積回路は、カードに搭載されており、
前記半導体回路は、通信回線、並びに当該通信回線に接続された通信装置を介して前記集積回路にアクセスを行う請求項８に記載のデータ処理方法。
【請求項９】前記第３の階層には、前記集積回路を用いた取り引きを行う複数の事業者のそれぞれに対応したアプリケーションプログラムが属し、当該複数のアプリケーションプログラムのそれぞれにファイアウォールが規定されており、前記ファイアウォールを介した前記アプリケーションプログラム間のデータ授受またはデータ参照が規制されている請求項８に記載のデータ処理方法。
【請求項１０】前記認証用装置は、当該認証用装置に加えられた物理的な外力であって前記アクセス原鍵情報が不正に操作される可能性がある外力を検出した場合に、前記記憶しているアクセス原鍵情報を自動的に消去する請求項２に記載のデータ処理方法。
【請求項１１】複数の階層からなるソフトウェア構造を有する半導体回路であって、
各階層に対応したダウンロード用署名検証鍵情報を参照可能であり、ダウンロード要求を受けると、当該ダウンロード要求に対応して生成されたダ
ウンロード用署名情報を、前記ダウンロード用署名検証鍵情報を用いて検証し、
前記ダウンロード用署名情報が正当であると検証したことを条件に、当該検証に用いたダウンロード用署名検証鍵情報に対応した階層のプログラムを、当該半導体回路または当該半導体回路にアクセス可能な半導体記憶回路にダウンロードすることを、前記ダウンロード要求の発行元に許可する半導体回路。
【請求項１２】前記半導体回路のソフトウェア構造が、前記半導体回路の管理者にのみダウンロード権が与えられた第１の階層と、前記第１の階層の上位に位置し所定の集積回路を操作するプログラムが属する第２の階層と、前記第２の階層の上位に位置し前記集積回路を用いた取り引き手続き内容を規定したアプリケーションプログラムが属する第３の階層とに分類されている請求項１２に記載の半導体回路。
【請求項１３】前記集積回路は、カードに搭載されてお

り、
前記半導体回路は、通信回線、並びに当該通信回線に接続された通信装置を介して前記集積回路にアクセスを行う請求項１３に記載の半導体回路。
【請求項１４】前記第３の階層には、前記集積回路を用いた取り引きを行う複数の事業者のそれぞれに対応したアプリケーションプログラムが属し、当該複数のアプリケーションプログラムのそれぞれにファイアウォールが規定されており、前記ファイアウォールを介した前記アプリケーションプログラム間のデータ授受またはデータ参照が規制されている請求項１４に記載の半導体回路。
【請求項１５】複数の階層からなるソフトウェア構造を有する半導体回路または当該半導体回路がアクセス可能な半導体記憶装置に、前記半導体回路内で動作するプログラムをダウンロードする際の認証に用いられる認証用装置であって、
前記ダウンロードが許可されるプログラムが属する前記階層に対応したアクセス原鍵情報を記憶し、
前記半導体回路に前記ダウンロード要求を送信し、
当該アクセス原鍵情報を用いて前記ダウンロード用署名情報を生成し、当該ダウンロード用署名情報を前記半導体回路に送信する認証用装置。
【請求項１６】前記半導体回路の識別情報を記憶し、
前記識別情報を平文として前記アクセス原鍵情報を用いて暗号化を行ってダウンロード用原鍵情報を生成し、当該ダウンロード用原鍵情報を用いて前記ダウンロード用署名情報を生成する請求項１６に記載の認証用装置。
【請求項１７】前記半導体回路へのダウンロードを許可された前記階層に対応する第１のアクセス原鍵情報、並びに、当該階層の上位の単数または複数の階層にそれぞれ対応した単数または複数の第２のアクセス原鍵情報を記憶し、
前記第１のアクセス原鍵情報、並びに前記単数または複数の第２のアクセス原鍵情報を用いて前記ダウンロード用署名情報を生成する請求項１７に記載の認証用装置。
【請求項１８】前記半導体回路との間で相互認証を行った後に、前記ダウンロード用署名情報を前記半導体回路に送信する請求項１７に記載の認証用装置。
【請求項１９】相互認証用原鍵情報、並びに前記半導体回路の識別情報を記憶し、
前記識別情報を平文として前記相互認証用原鍵情報を用いて暗号化を行って相互認証用鍵情報を生成し、
前記相互認証用鍵情報を用いて前記半導体回路との間で相互認証を行う請求項１９に記載の認証用装置。
【請求項２０】当該認証用装置に加えられた物理的な外力であって前記アクセス原鍵情報が不正に操作される可能性がある外力を検出した場合に、前記記憶しているアクセス原鍵情報を自動的に消去する請求項１６に記載の認証用装置。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】本発明は、半導体回路へのプログラムのダウンロードを所定の権限を有する者にのみ認めるデータ処理方法、半導体回路および認証用装置に関する。
【０００２】
【従来の技術】現在、ＩＣカードを用いてインターネットなどのネットワークを介した取り引きを行う通信システムが開発されている。このような通信システムでは、決済を行うサーバ装置が、例えばＩＣカードのリーダ・ライタやＰＣ(Personal Computer）からＩＣカードを用いた処理要求を受け、ユーザ認証やデータの暗号化及び復号などの処理を行う。サーバ装置上には、例えば、複数のクレジットカード会社などの事業者のアプリケーションプログラムが動作している。このようなアプリケーションプログラムは、各事業者が作成し、パーソナルコンピュータなどからサーバ装置にダウンロードする。また、各事業者は、アプリケーションプログラムをサーバ装置にダウンロードした後に、必要に応じてデバックなどを行う。
【０００３】
【発明が解決しようとする課題】しかしながら、上述したように各事業者がサーバ装置にアプリケーションプログラムをダウンロードしたり、当該アプリケーションプログラムのデバックなどを行う場合に、サーバ装置内のプログラムが不正に改竄等されることを防止する必要がある。これを実現する手法として、例えば、サーバ装置へのアクセスを行う際に、鍵情報を用いた認証処理を行う手法があるが、通常、このような鍵情報は端末装置（上記パーソナルコンピュータ）のメモリに記憶されているため、不正利用される可能性があり、セキュリティ上の問題がある。
【０００４】本発明は、上述した従来技術に鑑みてなされたものであり、サーバ装置などの半導体回路へのアクセス内容をその権限に応じて規制できるデータ処理方法、半導体回路および認証用装置を提供することを目的とする。
【０００５】
【課題を解決するための手段】上述した目的を達成するために、本発明のデータ処理方法は、半導体回路または当該半導体回路がアクセス可能な半導体記憶装置に、前記半導体回路内で動作するプログラムをダウンロードするデータ処理方法であって、前記半導体回路が複数の階層からなるソフトウェア構造を有し、各階層に対応したダウンロード用署名検証鍵情報を前記半導体回路が参照可能であり、前記半導体回路がダウンロード要求を受けると、当該ダウンロード要求に対応して生成されたダウンロード用署名情報を、前記ダウンロード用署名検証鍵情報を用いて検証し、前記ダウンロード用署名情報が正当であると検証したことを条件に、当該検証に用いたダ

ウンロード用署名検証鍵情報に対応した階層プログラムのダウンロードを、前記ダウンロード要求の発行元に許可する。

【０００６】また、本発明のデータ処理方法は、好ましくは、認証用装置が、ダウンロードが許可されるプログラムが属する階層に対応したアクセス原鍵情報を記憶し、前記認証用装置が、前記半導体回路に前記ダウンロード要求を送信し、前記認証用装置が、当該アクセス原鍵情報を用いて前記ダウンロード用署名情報を生成し、当該ダウンロード用署名情報を前記半導体回路に送信する。

【０００７】また、本発明のデータ処理方法は、好ましくは、前記認証用装置が、前記半導体回路の識別情報を記憶し、前記認証用装置が、前記識別情報を平文として前記アクセス原鍵情報を用いて暗号化を行ってダウンロード用源鍵情報を生成し、当該ダウンロード用原鍵情報を用いて前記ダウンロード用署名情報を生成する。

【０００８】また、本発明のデータ処理方法は、好ましくは、前記認証用装置が、前記半導体回路へのダウンロードを許可された前記階層に対応する第１のアクセス原鍵情報、並びに、当該階層の上位の単数または複数の階層にそれぞれ対応した単数または複数の第２のアクセス原鍵情報を記憶し、前記認証用装置が、前記第１のアクセス原鍵情報、並びに前記単数または複数の第２のアクセス原鍵情報を用いて前記ダウンロード用署名情報を生成する。

【０００９】また、本発明のデータ処理方法は、好ましくは、前記認証用装置は、前記半導体回路との間で相互認証を行った後に、前記ダウンロード用署名情報を前記半導体回路に送信する。

【００１０】また、本発明のデータ処理方法は、好ましくは、前記認証用装置が、相互認証用原鍵情報、並びに前記半導体回路の識別情報を記憶し、前記認証用装置が、前記識別情報を平文として前記相互認証用原鍵情報を用いて暗号化を行って相互認証用鍵情報を生成し、前記認証用装置が、前記相互認証用鍵情報を用いて前記半導体回路との間で相互認証を行う。

【００１１】また、本発明のデータ処理方法は、好ましくは、前記半導体回路のソフトウェア構造が、前記半導体回路の管理者にのみダウンロード権が与えられた第１の階層と、前記第１の階層の上位に位置し所定の集積回路を操作するプログラムが属する第２の階層と、前記第２の階層の上位に位置し前記集積回路を用いた取り引き手続き内容を規定したアプリケーションプログラムが属する第３の階層とに分類されている。

【００１２】また、本発明のデータ処理方法は、好ましくは、前記集積回路は、カードに搭載されており、前記半導体回路は、通信回線、並びに当該通信回線に接続された通信装置を介して前記集積回路にアクセスを行う。

【００１３】また、本発明のデータ処理方法は、好ましくは、前記第３の階層には、前記集積回路を用いた取り引きを行う複数の事業者のそれぞれに対応したアプリケーションプログラムが属し、当該複数のアプリケーションプログラムのそれぞれにファイアウォールが規定されており、前記ファイアウォールを介した前記アプリケーションプログラム間のデータ授受またはデータ参照が規制されている。

【００１４】また、本発明のデータ処理方法は、好ましくは、前記認証用装置は、当該認証用装置に加えられた物理的な外力であって前記アクセス原鍵情報が不正に操作される可能性がある外力を検出した場合に、前記記憶しているアクセス原鍵情報を自動的に消去する。

【００１５】また、本発明の半導体回路は、複数の階層からなるソフトウェア構造を有する半導体回路であって、各階層に対応したダウンロード用署名検証鍵情報を参照可能であり、ダウンロード要求を受けると、当該ダウンロード要求に対応して生成されたダウンロード用署名情報を、前記ダウンロード用署名検証鍵情報を用いて検証し、前記ダウンロード用署名情報が正当であると検証したことを条件に、当該検証に用いたダウンロード用署名検証鍵情報に対応した階層のプログラムを、当該半導体回路または当該半導体回路にアクセス可能な半導体記憶回路にダウンロードすることを、前記ダウンロード要求の発行元に許可する。

【００１６】また、本発明の認証用装置は、複数の階層からなるソフトウェア構造を有する半導体回路または当該半導体回路がアクセス可能な半導体記憶装置に、前記半導体回路内で動作するプログラムをダウンロードする際の認証に用いられる認証用装置であって、前記ダウンロードが許可されるプログラムが属する前記階層に対応したアクセス原鍵情報を記憶し、前記半導体回路に前記ダウンロード要求を送信し、当該アクセス原鍵情報を用いて前記ダウンロード用署名情報を生成し、当該ダウンロード用署名情報を前記半導体回路に送信する。

【００１７】

【発明の実施の形態】以下、本発明の実施の形態を添付図面を参照して説明する。図１は、本実施形態の通信システム３０１の全体構成図である。図１に示すように、通信システム３０１は、サーバ装置３０２、ＩＣカード３０３（本発明の集積回路）、カードリーダ・ライタ３０４、パーソナルコンピュータ３０５、ＡＳＰ(Application Service Provider)サーバ装置１０６、ＳＡＭ(Secure Application Module) ユニット３０９、パーソナルコンピュータ３１６＿１，３１６＿２，３１６＿３，３１６＿４，３１６＿５、認証用ユニット３１７＿１，３１７＿２，３１７＿３，３１７＿４，３１７＿５（本発明の認証用装置）、並びにＩＣＥ(In Circuit Emulator) ３１８を用いて、インターネット３１０を介して通信を行って、ＳＡＭチップ３０８のソフトウェアの開発やカスタマイズ、並びにＩＣカード３０３を用いた決済

処理などを行う。ＳＡＭユニット３０９は、外部メモリ３０７（本発明の半導体記憶回路）およびＳＡＭチップ３０８（本発明の半導体回路）を有する。ＳＡＭチップ３０８は、図２に示すようなソフトウェア構成を有している。図２に示すように、ＳＡＭチップ３０８は、下層から上層に向けて、HW(Hardware)層、ＯＳ層、下位ハンドラ層、上位ハンドラ層およびアプリケーション（ＡＰ）層を順に有している。下位ハンドラ層は、アプリケーションプログラムに依存しない処理を規定する層であり、ＯＳＩプロトコルにおけるトランスポート層、ネットワーク層およびデータリンク層に対応している。下位ハンドラ層には、ドライバ層が含まれる。ドライバ層は、ＬＳＩの操作に係わる処理を行う層である。上位ハンドラ層は、アプリケーションプログラムに依存する処理を規定する層であり、ＯＳＩプロトコルにおけるトランスポート層より上の層に対応している。ここで、ＯＳ層が本発明の第１の層に対応し、下位ハンドラ層、ドライバ層および上位ハンドラ層が本発明の第２の層に対応し、ＡＰ層が本発明の第３の層に対応している。

【００１８】ＡＰ層には、図１に示すクレジットカード会社などの事業者３１５＿１，３１５＿２，３１５＿３によるＩＣカード３０３を用いた手続きを規定したアプリケーションプログラムＡＰ＿１，ＡＰ＿２，ＡＰ＿３がある。ＡＰ層では、アプリケーションプログラムＡＰ＿１，ＡＰ＿２，ＡＰ＿３相互間、並びに上位ハンドラ層との間にファイアウォールＦＷ（本発明のファイアウォール）が設けられている。

【００１９】図２に示すソフトウェア構造において、ＡＰ層で各事業者に特有の処理、例えばＩＣカード３０３を用いた決済処理の内容が規定されており、ＩＣカード３０３を直接操作する処理は上位ハンドラ層以下の層に規定されている。

【００２０】ＳＡＭチップ３０８は、ＳＣＳＩまたはＥｔｈｅｒｎｅｔなどを介してＡＳＰサーバ装置３０６に接続される。ＡＳＰサーバ装置３０６は、インターネット３１０を介して、パーソナルコンピュータ３０５，３１６＿１，３１６＿２，３１６＿３，３１６＿４，３１６＿５が接続されている。

【００２１】パーソナルコンピュータ３１６＿１は、ＳＡＭチップ３０８で実行されるアプリケーションプログラムＡＰ＿１の事業者３１５＿ＡＰ１が使用する。パーソナルコンピュータ３１６＿２は、ＳＡＭチップ３０８で実行されるアプリケーションプログラムＡＰ＿２の事業者３１５＿ＡＰ２が使用する。パーソナルコンピュータ３１６＿３は、ＳＡＭチップ３０８で実行されるアプリケーションプログラムＡＰ＿３の事業者３１５＿ＡＰ３が使用する。パーソナルコンピュータ３１６＿４は、ＳＡＭチップ３０８の図２に示す上位ハンドラ層、並びにドライバ層を含む下位ハンドラ層を開発可能なソフトウェア開発者３１５＿ＭＩＤが使用する。パーソナルコンピュータ３１６＿５は、ＳＡＭチップ３０８の製造元であり、ＳＡＭチップ３０８を統括して管理する権限を有するソフトウェア開発者３１５＿ＳＵＰが使用する。

【００２２】事業者３１５＿ＡＰ１，３１５＿ＡＰ２，３１５＿ＡＰ３は、パーソナルコンピュータ３１６＿１，３１６＿２，３１６＿３を用いてアプリケーションプログラムＡＰ＿１，ＡＰ＿２，ＡＰ＿３を作成し、それぞれ認証用ユニット３１７＿１，３１７＿２，３１７＿３を介して、当該作成したアプリケーションプログラムをＳＡＭチップ３０８を介して外部メモリ３０７内の予め割り当てられた記憶領域にダウンロードする。このとき、事業者３１５＿ＡＰ１，３１５＿ＡＰ２，３１５＿ＡＰ３は相互に無関係の者であるため、アプリケーションプログラムＡＰ＿１，ＡＰ＿２，ＡＰ＿３をダウンロードできる外部メモリ３０７内の記憶領域は予め決められており、当該記憶領域へのダウンロードを行う権限を有するか否かがＳＡＭチップ３０８によって検証される。また、アプリケーションプログラムＡＰ＿１，ＡＰ＿２，ＡＰ＿３の実行中は、ファイアウォールＦＷによって、アプリケーションプログラムＡＰ＿１，ＡＰ＿２，ＡＰ＿３の間でのデータの授受および参照が制限されている。

【００２３】ソフトウェア開発者３１５＿ＭＩＤは、認証用ユニット３１７＿４を介して、必要に応じて、ＳＡＭチップ３０８の図２に示す上位ハンドラ層、並びにドライバ層を含む下位ハンドラ層のカスタマイズ等のために所定のプログラムをＳＡＭチップ３０８にダウンロードする。

【００２４】ソフトウェア開発者３１５＿ＳＵＰは、認証用ユニット３１７＿５を介して、図２に示す全ての層のカスタマイズ等のために所定のプログラムをＳＡＭチップ３０８にダウンロードする。

【００２５】認証用ユニット３１７＿１～３１７＿５は、後述するように、それぞれパーソナルコンピュータ３１６＿１～３１６＿５から所定のプログラムをＳＡＭチップ３０８にダウンロードする際に、ＳＡＭチップ３０８との間で相互認証、並びにダウンロード用署名検証鍵情報の作成などを行う。

【００２６】パーソナルコンピュータ３０５は、例えば、ＩＣカード３０３の所有者であるエンドユーザが使用する。パーソナルコンピュータ３０５は、例えば、シリアルまたはＵＳＢを介してＤｕｍｂ型のカードリーダ・ライタ３０４に接続されている。カードリーダ・ライタ３０４が、ＩＣカード３０３との間で物理レベルに相当する例えば無線通信を実現する。ＩＣカード３０３への操作コマンドおよびＩＣカード３０３からのリスポンスパケットは、ＳＡＭユニット３０９側で生成および解読される。よって、その中間に介在するカードリーダ・ライタ３０４、パーソナルコンピュータ３０５およびＡＳＰサーバ装置３０６は、コマンドやリスポンス内容を

データペイロード部分に格納して中継する役割を果たすのみで、ＩＣカード３０３内のデータの暗号化や復号および認証などの実操作には関与しない。また、ＩＣＥ３１８は、ＳＡＭチップ３０８上で動作するプログラムをデバックする際などに用いられるエミュレータである。

【００２７】以下、図１に示す構成要素について説明する。

ＩＣカード３０３

ＩＣカード３０３は、ＳＡＭチップ３０８を用いた決済処理に必要な鍵情報などを記憶する。

【００２８】認証用ユニット３１７＿１～３１７＿５

図３は、認証用ユニット３１７＿１の機能ブロック図である。図３に示すように、認証用ユニット３１７＿１は、記憶部３５０＿１および処理部３５１＿１を有する。図３に示すように、記憶部３５０＿１は、ＳＡＭ＿ＩＤ、相互認証用原鍵情報Ｋ１およびアクセス原鍵情報ＫＡを記憶している。ＳＡＭ＿ＩＤは、ＳＡＭチップ３０８の識別情報である。相互認証用原鍵情報Ｋ１は、後述するように相互認証用鍵情報Ｋ２を生成するために用いられる。アクセス原鍵情報ＫＡは、後述するように、外部メモリ３０７にプログラムをダウンロードするときに用いられるダウンロード用署名情報を生成するために用いられる。アクセス原鍵情報ＫＡは、図２に示すＳＡＭチップ３０８のソフトウェア構造のＡＰ層のプログラムを外部メモリ３０７にダウンロードするために必要な鍵情報である。

【００２９】処理部３５１＿１は、図３に示すように、相互認証部３５２＿１およびダウンロード処理部３５３＿１を有する。相互認証部３５２＿１は、図４に示すように、プログラムを外部メモリ３０７にダウンロードする際に、ＳＡＭ＿ＩＤを平文として相互認証用原鍵情報Ｋ１を用いて暗号化を行って相互認証用鍵情報Ｋ２を生成し、当該相互認証鍵情報Ｋ２を用いてＳＡＭチップ３０８との間で相互認証を行う。ダウンロード処理部３５３＿１は、プログラムを外部メモリ３０７にダウンロードする際に、図５に示すように、ＳＡＭ＿ＩＤを平文としてアクセス原鍵情報ＫＡを用いて暗号化を行って、ダウンロード用鍵情報Ｋ＿ＤＡを生成する。また、ダウンロード処理部３５３＿１は、ダウンロード用鍵情報Ｋ＿ＤＡを用いてダウンロード用署名情報を生成し、これをＳＡＭチップ３０８に送信する。

【００３０】認証用ユニット３１７＿２，３１７＿３は、上述した認証用ユニット３１７＿１と同じ構成をしている。但し、例えば、アクセス原鍵情報ＫＡの内容は各認証用ユニットで異なる。

【００３１】図６は、認証用ユニット３１７＿４の機能ブロック図である。図６に示すように、認証用ユニット３１７＿４は、記憶部３５０＿４および処理部３５１＿４を有する。図６に示すように、記憶部３５０＿４は、ＳＡＭ＿ＩＤ、相互認証用原鍵情報Ｋ１およびアクセス原鍵情報ＫＡ，ＫＭを記憶している。ＳＡＭ＿ＩＤ、相互認証用原鍵情報Ｋ１およびアクセス原鍵情報ＫＡは、前述したものと同じである。アクセス原鍵情報ＫＭは、図２に示すＳＡＭチップ３０８のソフトウェア構造の上位ハンドラ層、並びにドライバ層を含む下位ハンドラ層のプログラムを外部メモリ３０７あるいはＳＡＭチップ３０８にダウンロードするために必要な鍵情報である。

【００３２】処理部３５１＿４は、図６に示すように、相互認証部３５２＿４およびダウンロード処理部３５３＿４を有する。相互認証部３５２＿４は、前述した図４に相互認証部３５２＿１と同じである。ダウンロード処理部３５３＿４は、プログラムを外部メモリ３０７にダウンロードする際に、図７に示すように、ＳＡＭ＿ＩＤを平文としてアクセス原鍵情報ＫＡを用いて暗号化を行って、ダウンロード用鍵情報Ｋ＿ＤＡを生成する。次に、ダウンロード処理部３５３＿４は、ダウンロード用鍵情報Ｋ＿ＤＡを平文としてアクセス原鍵情報ＫＭを用いて暗号化を行って、ダウンロード用鍵情報Ｋ＿ＤＭを生成する。次に、ダウンロード処理部３５３＿４は、ダウンロード用鍵情報Ｋ＿ＤＭを用いてダウンロード用署名情報を生成し、これをＳＡＭチップ３０８に送信する。

【００３３】図８は、認証用ユニット３１７＿５の機能ブロック図である。図８に示すように、認証用ユニット３１７＿５は、記憶部３５０＿５および処理部３５１＿５を有する。図８に示すように、記憶部３５０＿５は、ＳＡＭ＿ＩＤ、相互認証用原鍵情報Ｋ１およびアクセス原鍵情報ＫＡ，ＫＭ，ＫＳを記憶している。ＳＡＭ＿ＩＤ、相互認証用原鍵情報Ｋ１およびアクセス原鍵情報ＫＡ，ＫＭは、前述したものと同じである。アクセス原鍵情報ＫＳは、図２に示すＳＡＭチップ３０８のソフトウェア構造のＯＳ層のプログラムを外部メモリ３０７あるいはＳＡＭチップ３０８にダウンロードするために必要な鍵情報である。

【００３４】処理部３５１＿５は、図８に示すように、相互認証部３５２＿５およびダウンロード処理部３５３＿５を有する。相互認証部３５２＿５は、前述した図４に相互認証部３５２＿１と同じである。ダウンロード処理部３５３＿５は、プログラムを外部メモリ３０７にダウンロードする際に、図９に示すように、ＳＡＭ＿ＩＤを平文としてアクセス原鍵情報ＫＡを用いて暗号化を行って、ダウンロード用鍵情報Ｋ＿ＤＡを生成する。次に、ダウンロード処理部３５３＿５は、ダウンロード用鍵情報Ｋ＿ＤＡを平文としてアクセス原鍵情報ＫＭを用いて暗号化を行って、ダウンロード用鍵情報Ｋ＿ＤＭを生成する。次に、ダウンロード処理部３５３＿５は、ダウンロード用鍵情報Ｋ＿ＤＭを平文としてアクセス原鍵情報ＫＳを用いて暗号化を行って、ダウンロード用鍵情報Ｋ＿ＤＳを生成する。次に、ダウンロード処理部３５３＿５は、ダウンロード用鍵情報Ｋ＿ＤＳを用いてダウ

ンロード用署名情報を生成し、これをＳＡＭチップ３０８に送信する。

【００３５】本実施形態では、認証用ユニット３１７＿１，３１７＿４，３１７＿５は、記憶部３５０＿１，３５０＿４，３５０＿５内にセキュアな状態で情報を記憶しており、当該ユニットが外的な要因で破壊されたり、こじ開けられた場合には、そのことを検出部によって検出して、記憶部３５０＿１，３５０＿４，３５０＿５の記憶情報を消去する。

【００３６】ＳＡＭユニット３０９

〔外部メモリ３０７〕図１０は、外部メモリ３０７の記憶領域を説明するための図である。図１０に示すように、外部メモリ３０７の記憶領域には、事業者３１５＿１のアプリケーションプログラムＡＰ＿１が記憶されるＡＰ記憶領域３２０＿１、事業者３１５＿２のアプリケーションプログラムＡＰ＿２が記憶されるＡＰ記憶領域３２０＿２、事業者３１５＿３のアプリケーションプログラムＡＰ＿３が記憶されるＡＰ記憶領域３２０＿３、並びにＳＡＭチップ３０８の管理者が使用するＡＰ管理用記憶領域３２１がある。

【００３７】ＡＰ記憶領域３２０＿１に記憶されているアプリケーションプログラムＡＰ＿１は、複数のプログラムモジュールによって構成されている。ＡＰ記憶領域３２０＿１へのアクセスは、ファイアウォールＦＷ＿１によって制限されている。ＡＰ記憶領域３２０＿２に記憶されているアプリケーションプログラムＡＰ＿２は、複数のプログラムモジュールによって構成されている。ＡＰ記憶領域３２０＿２へのアクセスは、ファイアウォールＦＷ＿２によって制限されている。ＡＰ記憶領域３２０＿３に記憶されているアプリケーションプログラムＡＰ＿３は、複数のプログラムモジュールによって構成されている。ＡＰ記憶領域３２０＿３へのアクセスは、ファイアウォールＦＷ＿３によって制限されている。本実施形態では、上記プログラムモジュールは、例えば、ＳＡＭユニット３０９の外部から外部メモリ３０７にダウンロードされる最小単位である。各アプリケーションプログラムを構成するプログラムモジュールの数は、対応する事業者が任意に決定できる。

【００３８】また、外部メモリ３０７に記憶されたアプリケーションプログラムＡＰ＿１，ＡＰ＿２，ＡＰ＿３は、スクランブルされており、ＳＡＭチップ３０８に読み込まれたときに、デスクランブルされる。また、アプリケーションプログラムＡＰ＿１，ＡＰ＿２，ＡＰ＿３は、例えば、それぞれ図１に示すパーソナルコンピュータ３１６＿１，３１６＿２，３１６＿３を用いて、事業者３１５＿１，３１５＿２，３１５＿３によって作成され、ＳＡＭチップ３０８を介して外部メモリ３０７にダウンロードされる。

【００３９】ＡＰ管理用記憶領域３２１へのアクセスは、ファイアウォールＦＷ＿４によって制限されている。なお、ファイアウォールＦＷ＿１，ＦＷ＿２，ＦＷ＿３，ＦＷ＿４は、図２に示すファイアウォールＦＷに対応している。ＡＰ管理用記憶領域３２１には、ＡＰ管理用データ３３０が記憶されている。ＡＰ管理用データ３３０には、例えば、ＳＡＭ＿ＩＤ、相互認証用鍵情報Ｋ２（または相互認証用原鍵情報Ｋ１）、ダウンロード用署名検証鍵情報Ｋ＿ＤＶＡ，ＫＤＶＭ，ＫＤＶＳがある。ここで、ダウンロード用署名検証鍵情報Ｋ＿ＤＶＡは、ダウンロード用鍵情報Ｋ＿ＤＡを用いて生成された署名情報の正当性を検証する鍵情報である。ダウンロード用署名検証鍵情報Ｋ＿ＤＶＭは、ダウンロード用鍵情報Ｋ＿ＤＭを用いて生成された署名情報の正当性を検証する鍵情報である。ダウンロード用署名検証鍵情報Ｋ＿ＤＶＳは、ダウンロード用鍵情報Ｋ＿ＤＳを用いて生成された署名情報の正当性を検証する鍵情報である。

【００４０】ダウンロード用署名検証鍵情報は、当該プログラムモジュールをＳＡＭチップ３０８を介して外部メモリ３０７にダウンロードするときに行われる署名検証に用いられる鍵情報である。

【００４１】〔ＳＡＭチップ３０８〕図１１は、図１に示すＳＡＭチップ３０８の機能ブロック図である。図１１に示すように、ＳＡＭチップ３０８は、ＡＳＰＳ通信インタフェース部３６０、外部メモリ通信インタフェース部３６１、バススクランブル部３６２、暗号・復号部３６３、記憶部３６４およびＣＰＵ３６５を有する。ＳＡＭチップ３０８は、耐タンパ性のモジュールである。

【００４２】ＡＳＰＳ通信インタフェース部３６０は、図１に示すＡＳＰサーバ装置３０６との間のデータ入出力に用いられるインタフェースである。外部メモリ通信インタフェース部３６１は、外部メモリ３０７との間のデータ入出力に用いられるインタフェースである。バススクランブル部３６２は、外部メモリ通信インタフェース部３６１を介してデータを外部メモリ３０７との間で入出力する際に、出力するデータをスクランブルし、入力したデータをデスクランブルする。暗号・復号部３６３は、データの暗号化、並びに暗号化されたデータの復号を行う。記憶部３６４は、ＣＰＵ３６５の処理に用いられるデータを記憶する。ＣＰＵ３６５は、ＳＡＭチップ３０８が行うアプリケーションプログラムの実行を含む様々を処理を、タスクなどの形態で処理を行う。ＣＰＵ３６５は、例えば、インターネット３１０を介したプログラムモジュールのダウンロード処理を行うダウンロード用タスク３６５ａを実行する。

【００４３】以下、ＣＰＵ３６５のダウンロード用タスク３６５ａによるプログラムモジュールのダウンロード動作について説明する。図１２は、当該ダウンロード動作を説明するためのフローチャートである。以下の実施形態では、事業者３１５＿ＡＰ１が、図２および図１０に示すアプリケーションプログラムＡＰ＿１のプログラムモジュールをダウンロードする場合の動作を例に挙げ

て説明する。
ステップＳＴ３０１：図１に示すパーソナルコンピュータ３１６＿１が、認証用ユニット３１７＿１、インターネット３１０、ＡＳＰサーバ装置３０６およびＩＣＥ３１８を介して、アプリケーションプログラムＡＰ＿１を構成するダウンロードを行おうとするプログラムモジュールのモジュール名を指定したダウンロード要求をＳＡＭチップ３０８に送信する。
【００４４】ステップＳＴ３０２：認証用ユニット３１７＿１の処理部３５１＿１の相互認証部３５２＿１が、図４に示すように、ＳＡＭ＿ＩＤを平文として相互認証用原鍵情報Ｋ１を用いて暗号化を行って相互認証用鍵情報Ｋ２を生成する。
【００４５】ステップＳＴ３０３：認証用ユニット３１７＿１の処理部３５１＿１の相互認証部３５２＿１が、ＳＡＭチップ３０８のＣＰＵ３６５のダウンロード用タスク３６５ａとの間で、ステップＳＴ３０２で生成した相互認証用鍵情報Ｋ２を用いて相互認証を行う。
【００４６】ステップＳＴ３０４：ステップＳＴ３０３の相互認証においてお互いの正当性が確認されると、ステップＳＴ３０５の処理に進む、そうでない場合には処理を終了する。
【００４７】ステップＳＴ３０５：図３に示す認証用ユニット３１７＿１の処理部３５１＿１のダウンロード処理部３５３＿１が、図５に示すように、ＳＡＭ＿ＩＤを平文としてアクセス原鍵情報ＫＡを用いて暗号化を行って、ダウンロード用鍵情報Ｋ＿ＤＡを生成する。
【００４８】ステップＳＴ３０６：ダウンロード処理部３５３＿１が、ステップＳＴ３０５で生成したダウンロード用鍵情報Ｋ＿ＤＡを用いてダウンロード用署名情報を生成する。
【００４９】ステップＳＴ３０７：ダウンロード処理部３５３＿１が、ステップＳＴ３０６で生成したダウンロード用署名情報をＳＡＭチップ３０８に送信する。
【００５０】ステップＳＴ３０８：図１１に示すＳＡＭチップ３０８のＣＰＵ３６５のダウンロード用タスク３６５ａが、図１０に示すダウンロード用署名検証鍵情報Ｋ＿ＤＶＡを用いて、ステップＳＴ３０７で受信したダウンロード用署名情報の正当性を判断する。このとき、ダウンロード用タスク３６５ａは、ステップＳＴ３０１で受信したモジュール名に基づいて、ダウンロード要求がＡＰ層について行われたと判断し、ダウンロード用署名検証鍵情報Ｋ＿ＤＶＡを特定する。
【００５１】ステップＳＴ３０９：ステップＳＴ３０８においてダウンロード用署名情報が正当であると判断されると、ステップＳＴ３１０の処理に進む、そうでない場合には処理を終了する。
【００５２】ステップＳＴ３１０：図１１に示すＳＡＭチップ３０８のＣＰＵ３６５のダウンロード用タスク３６５ａが、ステップＳＴ３０１で指定されたモジュール名に対応する外部メモリ３０７内のアドレスをモジュール管理用データ３３０を参照して特定し、当該特定した外部メモリ３０７上のアドレスに、パーソナルコンピュータ３１６＿１から受信したプログラムモジュールをダウンロードする。
【００５３】なお、ソフトウェア開発者３１５＿ＭＩＤが、図２に示す上位ハンドラ層および下位ハンドラ層のプログラムモジュールを外部メモリ３０７にダウンロードする場合には、ステップＳＴ３０５において図７を用いて説明した手順でダウンロード用鍵情報Ｋ＿ＤＭが生成され、これを用いてステップＳＴ３０６でダウンロード用署名情報が生成される。また、ステップＳＴ３０８で、ＳＡＭチップ３０８内で、図１０に示すダウンロード用署名検証鍵情報Ｋ＿ＤＶＭを用いて、ダウンロード用署名情報の検証が行われる。また、ソフトウェア開発者３１５＿ＳＵＰが、図２に示すＯＳ層のプログラムモジュールを外部メモリ３０７にダウンロードする場合には、ステップＳＴ３０５において図９を用いて説明した手順でダウンロード用鍵情報Ｋ＿ＤＳが生成され、これを用いてステップＳＴ３０６でダウンロード用署名情報が生成される。また、ステップＳＴ３０８で、ＳＡＭチップ３０８内で、図１０に示すダウンロード用署名検証鍵情報Ｋ＿ＤＶＳを用いて、ダウンロード用署名情報の検証が行われる。
【００５４】なお、ソフトウェア開発者３１５＿ＭＩＤ，３１５＿ＳＵＰは、アクセス原鍵情報ＫＡを用いて、ＡＰ層のプログラムモジュールを外部メモリ３０７にダウンロードできる。また、ソフトウェア開発者３１５＿ＳＵＰは、アクセス原鍵情報ＫＡ，ＫＭを用いて上位ハンドラ層および下位ハンドラ層のプログラムモジュールを外部メモリ３０７にダウンロードできる。
【００５５】以下、図１に示す通信システム３０１によるＩＣカード３０３を用いた取り引き処理について説明する。図１３は、図１に示す通信システム３０１の全体動作を説明するための図である。
ステップＳＴ３３１：事業者３１５＿１～３１５＿３あるいはこれら事業者の依頼を受けた者が、当該事業者がＩＣカード３０３を用いて行う取り引きについての処理を行うためのアプリケーションプログラムＡＰ＿１，ＡＰ＿２，ＡＰ＿３を、図１に示すパーソナルコンピュータ３１６＿１，３１６＿２，３１６＿３上で作成する。このとき図１２を用いて説明したダウンロード処理が行われる。
【００５６】ステップＳＴ３３２：アプリケーションプログラムＡＰ＿１，ＡＰ＿２，ＡＰ＿３を、認証用ユニット３１７＿１，３１７＿２，３１７＿３を介して、パーソナルコンピュータ３１６＿１，３１６＿２，３１６＿３からＳＡＭチップ３０８にダウンロードする。このとき、図９を用いて説明した処理が行われる。
【００５７】ステップＳＴ３３３：ユーザにＩＣカード

３０３が発行される。ＩＣカード３０３には、ユーザが契約を行った事業者との取り引きに用いられる鍵情報が記憶されている。なお、ユーザと事業者との間の契約は、ＩＣカード３０３の発行後に、インターネット３１０などを介して行ってもよい。

【００５８】ステップＳＴ３３４：例えば、ユーザがパーソナルコンピュータ３０５を用いてインターネット３１０を介してサーバ装置３０２にアクセスを行い、商品を購入しようとした場合に、サーバ装置３０２がインターネット３１０を介してＡＳＰサーバ装置３０６に処理要求を出す。ＡＳＰサーバ装置１０６は、サーバ装置３０２から処理要求を受けると、インターネット３１０を介してパーソナルコンピュータ３０５にアクセスを行う。そして、カードリーダ・ライタ３０４が出したＩＣカード３０３についての処理要求が、パーソナルコンピュータ３０５、インターネット３１０およびＡＳＰサーバ装置３０６を介してＳＡＭチップ３０８に送信される。

【００５９】ステップＳＴ３３５：ＳＡＭチップ３０８が、ステップＳＴ３３４で受信した処理要求に応じて、決済処理手順タスクによってアプリケーションプログラムを選択し、当該選択されたアプリケーションプログラムを実行する。

【００６０】ステップＳＴ３３６：ＳＡＭチップ３０８は、アプリケーションプログラムの実行結果をＡＳＰサーバ装置３０６に出力する。

【００６１】以上説明したように、通信システム３０１によれば、認証用ユニット３１７＿１，３１７＿２，３１７＿３がアクセス原鍵情報ＫＡを保持し、認証用ユニット３１７＿４がアクセス原鍵情報ＫＭを保持し、認証用ユニット３１７＿５がアクセス原鍵情報ＫＳを保持し、上述したように外部メモリ３０７へのプログラムモジュールのダウンロード処理を行うことで、図２に示すソフトウェア階層に応じて与えた権限に応じたプログラムモジュールのダウンロードが可能になる。そのため、権限の無い者によって、ＳＡＭチップ３０８で実行されるプログラムモジュールが不正に交換されたり、改竄されることを防止できる。

【００６２】また、通信システム３０１によれば、前述したように、認証用ユニット３１７＿１，３１７＿４，３１７＿５は、記憶部３５０＿１，３５０＿４，３５０＿５内にセキュアな状態で情報を記憶しており、当該ユニットが外的な要因で破壊されたり、こじ開けられた場合には、そのことを検出部によって検出して、記憶部３５０＿１，３５０＿４，３５０＿５の記憶情報を消去する。そのため、ＳＡＭチップ３０８へのダウンロードに用いられる鍵情報が不正に使用されることを回避できる。

【００６３】また、通信システム３０１によれば、ＳＡＭチップ３０８が複数のアプリケーションプログラムを動作させる場合に、アプリケーションプログラム間でのデータ授受やデータ・コードの参照をファイアウォールＦＷ＿１，ＦＷ＿２，ＦＷ＿３によって制限することから、各アプリケーションプログラムの処理が、他のアプリケーションプログラムによって不正干渉、改竄されることを防止できる。また、各アプリケーションプログラムの秘匿性を高めることができる。

【００６４】また、通信システム３０１によれば、各アプリケーションプログラムを複数のプログラムモジュールで構成することで、外部メモリ３０７に対してプログラムモジュール単位でダウンロードを行うことができる。

【００６５】また、通信システム３０１によれば、秘匿性の高いＩＣカード３０３に対しての操作に用いられる鍵情報を、通常行われるスクランブルに加えて、暗号化して外部メモリ３０７に格納することで、当該鍵情報のセキュリティレベルを向上できる。

【００６６】また、インターネット３０１によれば、アプリケーションプログラムは、バススクランブル機能によりコードアクセス時に暗号化・復号化を実行しているため、ＳＡＭチップ３０８の処理停止中に、外部メモリ３０７に記憶されたアプリケーションプログラムが不正に解析等されることを防止できる。

【００６７】図１４は、図１１に示すＳＡＭチップ３０８の機能ブロックをより具体的にした機能ブロック図である。図１４に示すように、ＳＡＭチップ３０８は、内部バス９０を介して、ＡＳＰＳ通信インタフェース部３６０、外部メモリ通信インタフェース部３６１、バススクランブル部３６２、暗号・復号部３６５、記憶部３６４およびＣＰＵ３６５が接続されている。

【００６８】図１４に示すＳＡＭチップ３０８では、例えば図１５に示すように、内部バス９０に接続されたカードＩ／Ｆ部９１を、ＳＡＭチップ３０８の外部のＲＦ送受信部９２に接続し、ＲＦ送受信部９２のアンテナ９２ａを介して、ＩＣカード３０３との間で非接触方式でデータを送受信してもよい。

【００６９】本発明は上述した実施形態には限定されない。例えば、上述した実施形態では、パーソナルコンピュータ３１６＿１～３１６＿５からＳＡＭチップ３０８を介して外部メモリ３０７にプログラムモジュールをダウンロードする場合を例示したが、本発明は、パーソナルコンピュータ３１６＿１～３１６＿５からＳＡＭチップ３０８内の記憶部３６４にプログラムモジュールをダウンロードする場合にも、上述したダウンロード用タスク３６５ａの機能を用いて同様に適用できる。

【００７０】また、上述した実施形態では、インターネット３１０に対してパーソナルコンピュータ３１６＿１～３１６＿５側に認証用ユニット３１７＿１～３１７＿５を設けた場合を例示したが、図１６に示すように、認証用ユニット３１７＿１～３１７＿５をＳＡＭチップ３

０８内に設け、認証用ユニット３１７＿１～３１７＿５をへのアクセスを対応するパーソナルコンピュータ３１６＿１～３１６＿５に対して許可するようにしてもよい。

【００７１】

【発明の効果】以上説明したように、本発明によれば、半導体回路で用いられるプログラムのダウンロードを、ダウンロード元に予め与えられた権限に応じて規定できるデータ処理方法、半導体回路および認証用装置を提供することができる。

【図面の簡単な説明】

【図１】図１は、本発明の実施形態の通信システムの全体構成図である。

【図２】図２は、図１に示すＳＡＭチップのソフトウェア構成を説明するための図である。

【図３】図３は、図１に示すアプリケーションプログラムを使用する事業者の認証用ユニットの機能ブロック図である。

【図４】図４は、図３に示す相互認証部の機能を説明するための図である。

【図５】図５は、図３に示すダウンロード処理部の機能を説明するための図である。

【図６】図６は、図１に示すハンドラ層のソフトウェア開発者の認証用ユニットの機能ブロック図である。

【図７】図７は、図６に示すダウンロード処理部の機能を説明するための図である。

【図８】図８は、図１に示すＳＡＭチップの管理者の認証用ユニットの機能ブロック図である。

【図９】図９は、図８に示すダウンロード処理部の機能を説明するための図である。

【図１０】図１０は、図１に示すＳＡＭユニットの外部メモリを説明するための図である。

【図１１】図１１は、図１に示すＳＡＭチップの機能ブロック図である。

【図１２】図１２は、図１に示すパーソナルコンピュータから、外部メモリにアプリケーションプログラムをダウンロードする動作を説明するためのフローチャートである。

【図１３】図１３は、図１に示す通信システムのＩＣカードを用いた取り引き処理を説明するための図である。

【図１４】図１４は、図１１に示すＳＡＭチップの機能ブロックをより具体的にした機能ブロック図である。

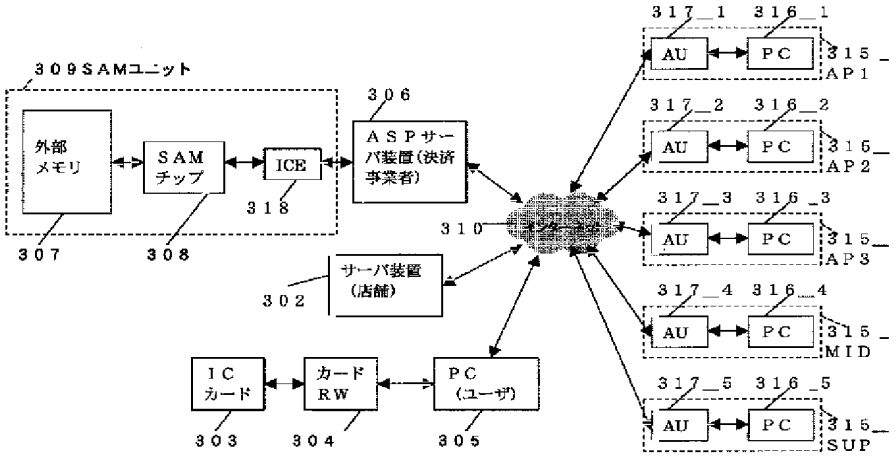
【図１５】図１５は、ＳＡＭチップのその他の使用形態を説明するための図である。

【図１６】図１６は、図１に示す通信システムの変形例を説明するための図である。

【符号の説明】

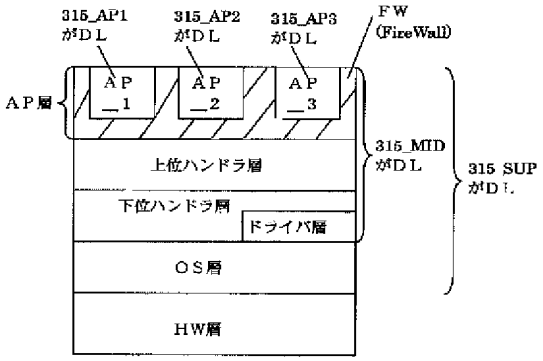
３０１…通信システム、３０２…サーバ装置、３０３…ＩＣカード、３０４…カードリーダ・ライタ、３０５…パーソナルコンピュータ、３０６…ＡＳＰサーバ装置、３０７…外部メモリ、３０８…ＳＡＭチップ、３０９…ＳＡＭユニット、３１０…インターネット、３１５＿１，３１５＿２，３１５＿３…クレジットカード事業者、３１５＿４…ハンドラ層の開発者、３１５＿５…ＳＡＭチップの管理者、３１６＿１～３１６＿５…パーソナルコンピュータ、３１７＿１～３１７＿５…認証用ユニット、３１８…ＩＣＥ

【図１】



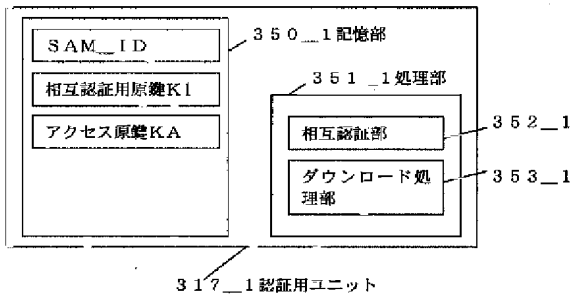
３０１

【図2】

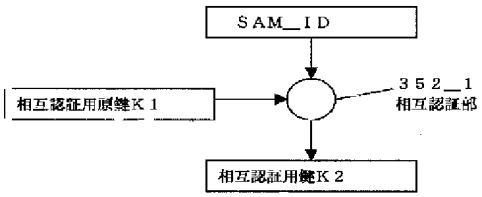


SAMチップのソフトウェア構成

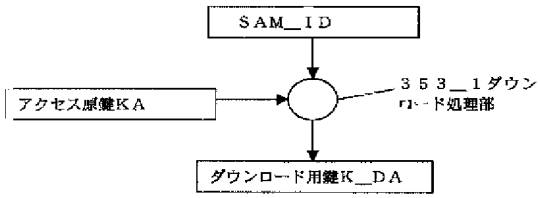
【図3】



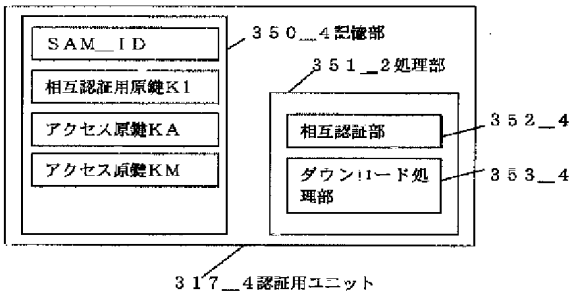
【図4】



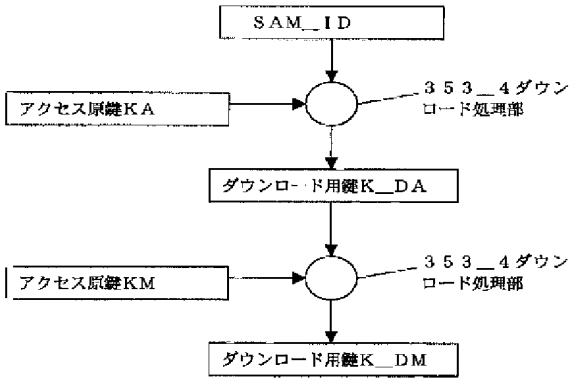
【図5】



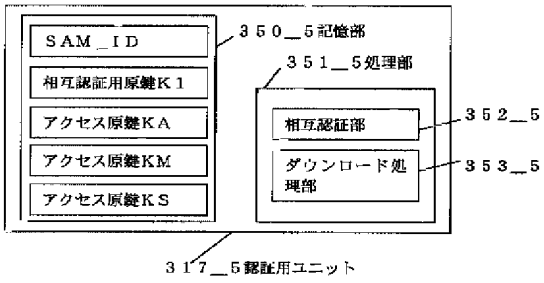
【図6】



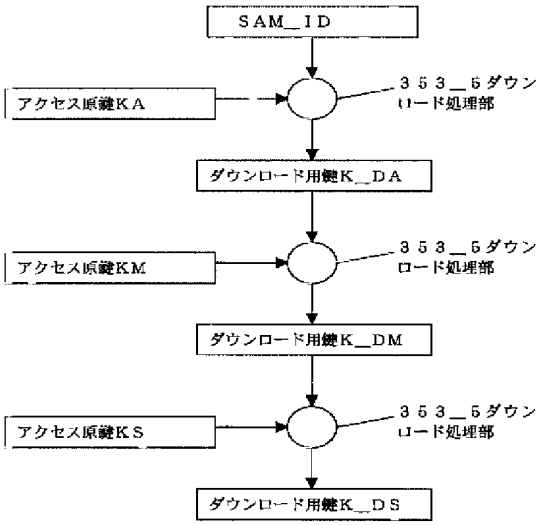
【図7】



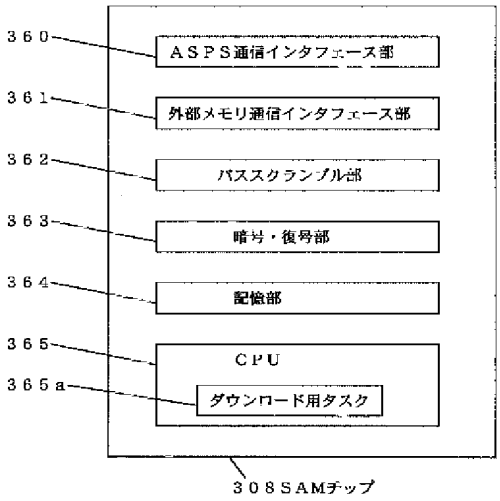
【図8】



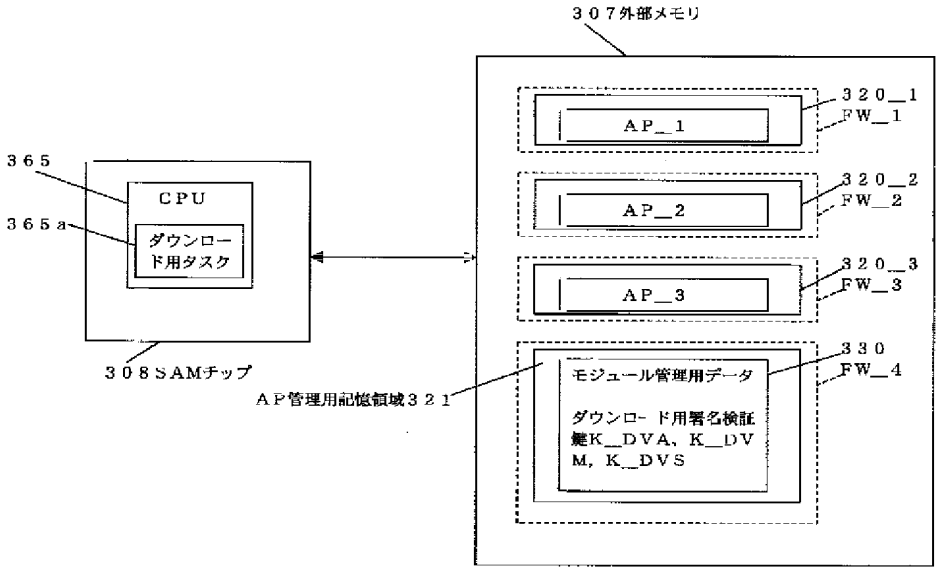
【図9】


SAM_ID
アクセス原鍵KA
353_5ダウンロード処理部
ダウンロード用鍵K_DA
アクセス原鍵KM
353_5ダウンロード処理部
ダウンロード用鍵K_DM
アクセス原鍵KS
353_5ダウンロード処理部
ダウンロード用鍵K_DS

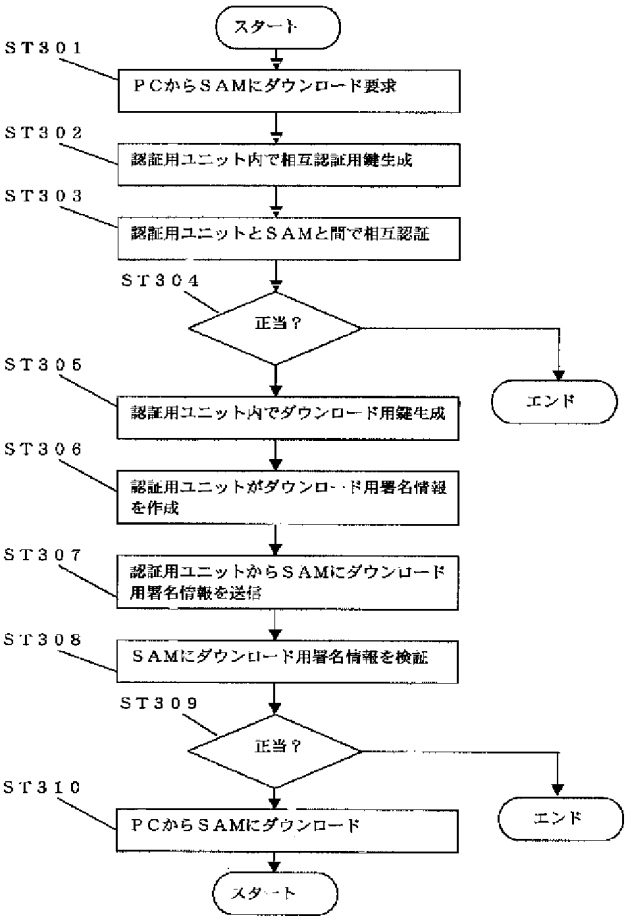
【図11】


360
ASPS通信インタフェース部
361
外部メモリ通信インタフェース部
362
パススクランブル部
363
暗号・復号部
364
記憶部
365
CPU
365a
ダウンロード用タスク
308SAMチップ

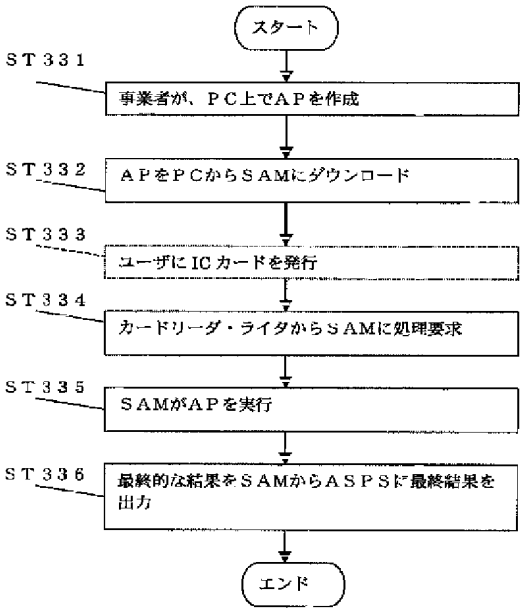
【図10】


307外部メモリ
320_1
FW_1
AP_1
320_2
FW_2
AP_2
320_3
FW_3
AP_3
330
FW_4
モジュール管理用データ
ダウンロード用署名検証鍵K_DVA, K_DVM, K_DVS
AP管理用記憶領域321
365
CPU
365a
ダウンロード用タスク
308SAMチップ

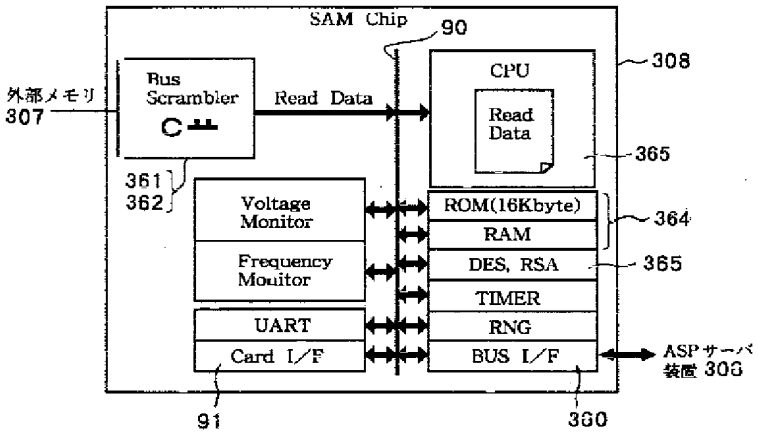
【図12】


スタート
ST301
PCからSAMにダウンロード要求
ST302
認証用ユニット内で相互認証用鍵生成
ST303
認証用ユニットとSAMと間で相互認証
ST304
正当？
エンド
ST305
認証用ユニット内でダウンロード用鍵生成
ST306
認証用ユニットがダウンロード用署名情報を作成
ST307
認証用ユニットからSAMにダウンロード用署名情報を送信
ST308
SAMにダウンロード用署名情報を検証
ST309
正当？
エンド
ST310
PCからSAMにダウンロード
スタート

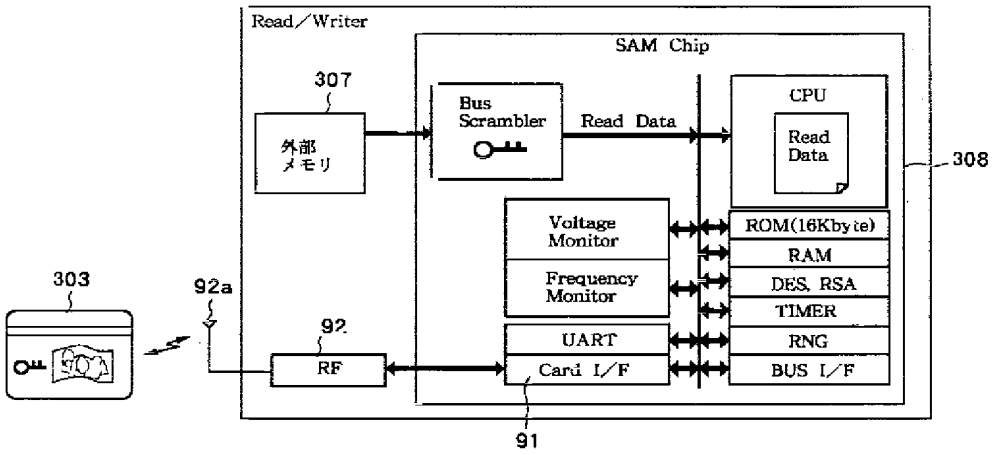
【図13】


スタート
ST331
事業者が、PC上でAPを作成
ST332
APをPCからSAMにダウンロード
ST333
ユーザにICカードを発行
ST334
カードリーダ・ライタからSAMに処理要求
ST335
SAMがAPを実行
ST336
最終的な結果をSAMからASPSに最終結果を出力
エンド

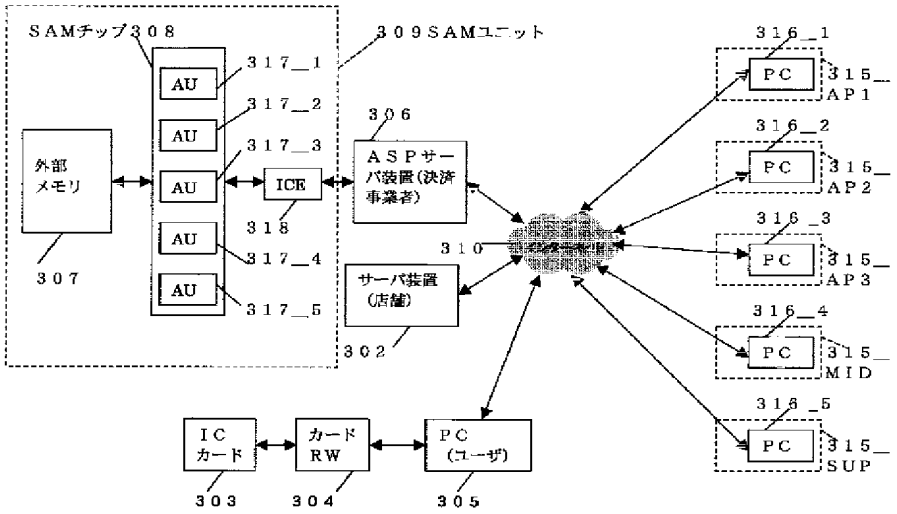
【図14】


SAM Chip
90
外部メモリ
307
Bus Scrambler
Read Data
CPU
Read Data
308
365
361
362
Voltage Monitor
Frequency Moultor
ROM(16Kbyte)
RAM
364
DES, RSA
365
TIMER
UART
RNG
Card I/F
BUS I/F
ASPサーバ装置 306
91
360

【図１５】



【図１６】



フロントページの続き

(51)Int.Cl.[7]		識別記号	FI		(参考)
G09C	1/00	640	G06K	19/00	N
					P
H04L	9/10		H04L	9/00	621A
	9/32				675A

Fターム(参考) 5B035 AA13 BB09 CA29 CA38
5B058 CA26 CA27 KA32 KA33
5B076 FB05 FC01 FD02
5J104 AA07 AA09 AA12 KA04 NA02
NA35 NA41 NA42 PA07 PA10